APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,809	02/27/2004	Trevor W. Freeman	MSI-1747US	5655

22801 7590 02/04/2008	EXAMINER	
LEE & HAYES PLLC	KAPLAN, BENJAMIN A	
421 W RIVERSIDE AVENUE SUITE 500		
SPOKANE, WA 99201	ART UNIT	PAPER NUMBER
	2139	

MAIL DATE	DELIVERY MODE
02/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _19 November 2007_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-5,7-13 and 15-34_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-5,7-13 and 15-34_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _27 February 2004_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _11/16/2007_.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This Office action is in regards to the most recent papers filed on 11/19/2007.

2.   Claims 1-5, 7-13 & 15-34 are pending.

3.   Claims 6 & 14 have been canceled.

4.   Claims 1, 9-13, 15, 16, 23, 27, 30 & 34 were amended.

5.   Claims 1-5, 7-13 & 15-34 are rejected.

Response to Arguments

6.   Applicant's arguments filed 10/26/2007 have been fully considered but they are

not persuasive.

7.   Applicant's arguments with respect to claims 16-22 have been considered but are

moot in view of the new ground(s) of rejection.

8.   In substance applicant argued that:

1) The rejection was dependent on the use of a secondary network.

With   the   definitions   provided   by   applicant   for   out-of-band   (Applicants

specification   paragraph   [0017])   and   computer-readable   medium   (Applicants

specification   paragraph   [0055])   the   use   of   a   secondary   network   would   explicitly   be

covered by the claims, excluding Claims 16-22.

2) **The proposed combination renders Cisco and COBAS unsatisfactory for their intended purposes as**

A) Cisco considers an out-of-band transmission to be cumbersome and that it does not scale to the size needed for large networks.

While Cisco did indicate out-of-band transmission to be cumbersome it only showed consideration to the out-of-band transmission being a direct telephone call or registered mail (Cisco, Page 2, Lines 36-38). The out-of-band transmission method provided by COBAS directly provide a solution to the cumbersomeness of the out-of-band methods considered by Cisco as well as being scaleable. Further Applicants claims are not limited to a large scale network.

B) COBAS uses the out-of-band transmission only for authentication.

The position and use of the correct encryption key would normally be considered part is part of being authenticated as a valid user. Some basic recognition of encryption keys in found in (COBAS pages 4-5). The core of the COBAS method is to instead of just working with one connection path "separate the access and authentication paths." (COBAS, Page 5, Paragraph 6, Line 1). As correct encryption keys are part of being the correct authenticated user they would sensibly be taken as part of the authentication path as apposed to the access path.

This also applies to the combination of COBAS and Pretty Good Privacy PGP for Personal Privacy, Version 5.0.

Claim Rejections - 35 USC § 112

9.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10.   Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 16 is considered indefinite for lines 5-6 which recite "a computer processor capable of writing ..." as saying capable of makes it unclear as to what is actually being claimed by the limitation.

Claim Rejections - 35 USC § 101

11.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-5, 7-8, 16-22 & 30-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-5, 7-8 & 30-34 are non-statutory because the computer readable medium can be any medium and in the specification paragraph [0055] specifically mentions signals, which are non-statutory.

Claims 16-22 are non-statutory because the apparatus encompasses a human being, (Applicants Amended Claim 16, Lines 7-8, "a method of transporting the out-of-

band computer readable storage medium to a second node") which is non-statutory.

See MPEP § 2105 Patentable Subject Matter - Living Subject Matter.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12.   Claims 16-18 & 22 are rejected under 35 U.S.C. 102(e) as being anticipated by

United States Patent Application Publication No.: US 2004/0002878 A1 (Maria Hinton).

As per Claim 16: Maria Hinton teaches:

- a computer-readable storage medium

(Maria Hinton, Figure 1B, Elements 124, 126 & 132).

(Maria Hinton, Paragraph [0031], "With reference now to FIG. 1B, a diagram

depicts a typical computer architecture of a data processing system, such as those

shown in FIG. 1A, in which the present invention may be implemented. Data processing

system 120 contains one or more central processing units (CPUs) 122 connected to

internal system bus 123, which interconnects random access memory (RAM) 124, read-

only memory 126, and input/output adapter 128, which supports various I/O devices,

such as printer 130, disk units 132, or other devices not shown, such as a audio output

system, etc. System bus 123 also connects communication adapter 134 that provides

access to communication link 136. User interface adapter 148 connects various user

devices, such as keyboard 140 and mouse 142, or other devices not shown, such as a

touch screen, stylus, microphone, etc. Display adapter 144 connects system bus 123 to

display device 146.").

- a computer processor capable of writing the local public/private key pair to an

out-of-band computer-readable storage medium

 (Maria Hinton, Figure 1B, Element 122).

 (Maria Hinton, Paragraph [0031], as seen above).

 In Addition see (Maria Hinton, Figure 1A, Element 113).

 And PDA connections discussed in (Maria Hinton, Paragraph [0029]).

- a key generator on a first node to generate a local public/private key pair

- a method of transporting the out-of-band computer readable storage medium to

a second node

- a shared secret generator on the second node to receive the public key from the

first node via the out-of-band computer-readable storage medium connection and

which is able to generate a shared secret using the local private key and the

public key received from the first node

 (Maria Hinton, Paragraphs [0045]-[0047], "Hence, as shown in this example and

explained in more detail further below, the present invention relies upon the fact that the

user has previously established an authentication relationship with at least one

authentication service provider and possibly a plurality of authentication service providers, which would be primarily an "out-of-band" process by which the user enrolls or subscribes with an authentication service provider for authentication/proof-of-identity services. A user may contract for different strengths of authentication, such as username/password, smart card, biometric, or digital certificate; in other words, the present invention is able to interoperate with a variety of underlying authentication schemes.

The present invention also relies upon the fact that an e-commerce service provider has previously established trust relationship with at least one authentication service provider and possibly a plurality of authentication service providers, which would be primarily an "out-of-band" process by which the e-commerce service provider and an authentication service provider engage in various types of agreements with respect to liability of each party concerning authentication/proof-of-identity services. An e-commerce service provider may contract for different strengths of authentication, and the present invention is able to interoperate with a variety of underlying authentication schemes.

As part of the process of establishing a trust relationship, the e-commerce service provider and the authentication service provider would engage in an out-of-band exchange of information that is used to establish a trust relationship, which may include a shared secret key, digital certificates, or some other form of information. This information is used to protect user proof-of-identity information that is presented by the e-commerce service provider to the authentication service provider during a user

transaction. Public-key techniques may be used to exchange this information, but because of the limitations of public-keys and associated certificates and the security requirements on a proof-of-identity as presented to an e-commerce service provider, secret keys are preferable, although the present invention is operable with a public-key-based technique.").

The use of encryption keys includes the generation of said encryption keys. The use of smart cards or previously seen Personal Digital Assistants (PDAs) would be a transportation the out-of-band computer readable storage medium between nodes.

As per Claim 17: The rejection of claim 16 is incorporated and further Maria Hinton teaches:

- the shared secret is symmetrical to a shared secret generated on the other node using the local public key and a private key corresponding to the other node

(Maria Hinton, Paragraph [0048], Lines 1-2 "A preferred embodiment uses a secret-key-based technique").

Maria Hinton recognizes the use of symmetrical encryption keys as preferred. Note secret-key-based techniques are symmetrical encryption.

As per Claim 18: The rejection of claim 16 is incorporated and further Maria Hinton teaches:

- the other node is a server

(Maria Hinton, Figure 1D).

Maria Hinton's invention deals with connecting to a server.

As per Claim 22: The rejection of claim 16 is incorporated and further the use of PDAs or smart cards as the out of band connection was already shown in the rejection of claim 16.

Claim Rejections - 35 USC § 103

13.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14.   Claim 19-21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maria Hinton in view of Official Notice.

As per Claim 19: The rejection of claim 16 is incorporated and further Maria Hinton does not explicitly teach the shared secret is generated by performing a Diffie-Hellman computation however Diffie-Hellman computations were well know in the art at the time of invention was made.

It would have been obvious to one of ordinary skill in the art to incorporate the use of a Diffie-Hellman computation in to the teachings of Maria Hinton as a Diffie-Hellman computation is a specific secret-key-based technique that would complete

Maria Hinton's generally preferred key technique (Maria Hinton, Paragraph [0048], Lines 1-2 "A preferred embodiment uses a secret-key-based technique").

As per Claims 20 & 21: The rejection of claim 16 is incorporated and further Maria Hinton does not explicitly teach encoding the secret value using the public key received from the other node, transmitting the encoded secret value to the other node and generating a shared secret by performing RSA computation however this RSA method was well know in the art at the time of invention was made

It would have been obvious to one of ordinary skill in the art to incorporate the use of a RSA method in to the teachings of Maria Hinton as a RSA method is a specific public-key-based technique that would complete Maria Hinton's acknowledged viable public-key-based technique. (Maria Hinton, Paragraph [0047], Lines 14-15 "secret keys are preferable, although the present invention is operable with a public-key-based technique").

15.   Claims 1-3, 7-11, 14-15, 30, 31 & 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Enhanced IP Services for Cisco Networks</u> (<u>Cisco</u>). In further view of <u>C.O.B.A.S. Centralized Out-Of-Band Authentication System</u> (<u>C.O.B.A.S.</u>).

As per Claim 1: <u>Cisco</u> teaches:

- A method for establishing a trust relationship with a remote node

(Cisco, Page 1, Paragraph 1, Lines 1-4 "IPsec is a fairly large collection of technologies that encompasses network and security protocols, cryptographic algorithms, and recommendations. IPsec is an architecture for building secure communications over untrusted networks and provides the security services listed in the following sections. These services are confidentiality, integrity, origin authentication, and anti-replay.").

- generating a local public value and a local private value on at least one node

(Cisco, Page 3, Line 31 "Alice and Bob are given numbers g and n. These are non-secret, publicly available numbers.").

(Cisco, Page 3, Lines 32-33 "Alice picks a large random number, x, calculates $A=g^x$ mod n, and sends this value, A, to Bob over an untrusted network. The value x is known only to Alice and is called Alice's secret.").

At the Alice node, g is the public value and x is the private value.

- receiving a public value from another node

(Cisco, Page 3, Lines 34-35 "Bob picks a large random number, y, calculates $B=g^y$ mod n, and sends this value, B, to Alice over the untrusted network. The value y is known only to Bob and is Bob's secret.").

At the Alice node, B is the public value received from the other node.

- generating a secret value using the local private value in combination with the public value received from the other node.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^x$ mod n.").

At the Alice node, the generated secret value is K_a.

Cisco does not explicitly teach:

- storing the public value on an out-of-band computer-readable medium

- transporting the out-of-band computer-readable medium to the other node

- the receiving the public value via the out-of-band computer-readable medium wherein the receiving is asynchronous to the generating

However C.O.B.A.S. in analogous art does teach the above limitations.

(C.O.B.A.S., Page 5, Paragraph 6 "The way to correct the fatal flaw is to separate the access and authentication paths. This can be done by having the authentication done via a separate network that the hacker does not have access to. This scheme is called Out-of-Band Authentication.").

Receiving the public value and generating the secret value are two related but separate events, one must finish for the other to start. Receiving and generating are inherently asynchronous.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate

authentication transactions such as key exchanges from interception, unauthorized

monitoring and man in the middle attacks.

As per Claim 2: The rejection of claim 1 is incorporated and further <u>Cisco</u> teaches:

- method is performed on both of a pair of nodes

> (<u>Cisco</u>, Page 3, Line 31 as seen in the rejection of claim 1).

> (<u>Cisco</u>, Page 3, Lines 32-33 as seen in the rejection of claim 1).

> (<u>Cisco</u>, Page 3, Lines 34-35 as seen in the rejection of claim 1).

> (<u>Cisco</u>, Page 3, Line 37 "Bob computes $K_b = A^y \mod n$.").

The corresponding values at the Bob node are: n is the public value, y is the

private value, A is the public value received from the other node, K_b is the generated

secret value.

- the secret values generated at both of the nodes are symmetric.

> (<u>Cisco</u>, Page 3, Line 38 "By virtue of an algebraic property of exponents, K_a and

K_b are equal").

As per Claim 3: The rejection of claim 2 is incorporated and further <u>Cisco</u> teaches:

- generating a secret value includes performing a Diffie-Hellman computation.

> (Cisco, Page 3, Line 3 "Using Diffie-Hellman to Agree on a Shared Key").

The computations used in the rejections of claims 1 and 2 are Diffie-Hellman computations.

As per Claim 7: The rejection of claim 1 is incorporated and further C.O.B.A.S. teaches:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

(C.O.B.A.S., Page 4, Lines 18-21 "The secret key can be stored on the user's computer or in a special hardware device called a "Token". A special case of a Token is a "Smart Card" which is a credit card sized plastic card with a microprocessor chip embedded in the card. Smart Cards require a reader on the computer where access is made.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 8: The rejection of claim 7 is incorporated and further C.O.B.A.S. teaches:

- external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

(C.O.B.A.S., Page 4, Lines 18-21 as seen in the rejection of claim 7).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 9: Claim 9 is the method claim of claim 1 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 10: The rejection of claim 9 is incorporated and further:

Claim 10 is the method claim of claim 2 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 2.

As per Claim 11: The rejection of claim 9 is incorporated and further:

Claim 11 is the method claim of claim 3 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 3.

As per Claim 15: The rejection of claim 9 is incorporated and further:

Claim 15 is the combination of the method claim of claim 7 and its dependent claim, claim 8 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claims 7 and 8.

As per Claim 30: Claim 30 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 31: The rejection of claim 30 is incorporated and further:

Claim 31 is the method claim of claim 3 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 3.

As per Claim 34: The rejection of claim 30 is incorporated and further:

Claim 34 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

16.   Claims 1, 4-9, 12-15, 30 & 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pretty Good Privacy™ PGP for Personal Privacy, Version 5.0 (PGP). In further view of Cisco and C.O.B.A.S..

As per Claim 1: PGP teaches:

- A method for establishing a trust relationship with a remote node

(<u>PGP</u>, Page 1, Lines 1-3 "With PGP™ for Personal Privacy, you can easily protect the privacy of your email messages and file attachments by encrypting them so that only those with the proper authority can decipher the information.").

- generating a local public value and a local private value on at least one node

(<u>PGP</u>, Page 3, Lines 9-10 "you need to generate a key pair consisting of a private key to which only you have access and a public key").

The public key is the public value; the private key is the private value.

- receiving a public value from another node

(<u>PGP</u>, Page 3, Lines 16-21 "After you have created a key pair, you can begin corresponding with other PGP users. To do so, you will need a copy of their public key and they will need a copy of your public key. Since your public key is just a block of text, it is really quite easy to trade keys with someone. You can either include your public key in an email message, copy it to a file or you can post it on a public key server where anyone can get a copy when they need it.").

The public key that is sent from an "other PGP user" is the received public value.

<u>PGP</u> does not explicitly teach:

- and generating a secret value using the local private value in combination with the public value received from the other node.

However <u>Cisco</u> in analogous art teaches the above limitation.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^x$ mod n.").

The generated secret value is K_a, X is the local private value, B is the public value from other node.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of PGP in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to include a cryptographically strong equation in the generation of a pseudo-random single-key/session key.

PGP and Cisco do not explicitly teach:

- storing the public value on an out-of-band computer-readable medium

- transporting the out-of-band computer-readable medium to the other node

- the receiving via the out-of-band computer-readable medium wherein the receiving is asynchronous to the generating

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 5, Paragraph 6 "The way to correct the fatal flaw is to separate the access and authentication paths. This can be done by having the authentication done via a separate network that the hacker does not have access to. This scheme is called Out-of-Band Authentication.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate

authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 4: The rejection of claim 1 is incorporated and further PGP teaches:

- retaining the secret value locally

It is inherently necessary to retain the secret value (single-key/session key) in order to take any further action using it or based on it.

- protecting the secret value using the public value received from the other node

(PGP, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

- transmitting the protected secret value to the other node

(PGP, Page 22, Lines 26-58 "Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and certified e-mail is create a new key pair.").

(PGP, Page 22, Lines 2-5 "Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit.").

<u>PGP</u> does not explicitly teach:

- via an out-of-band mechanism

However <u>C.O.B.A.S.</u> in analogous art does teach the above limitation.

    (<u>C.O.B.A.S.</u>, Page 5, Paragraph 6 as seen in the rejection of claim 1)

    It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of <u>C.O.B.A.S</u> in to the teachings of <u>Cisco</u>, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 5: The rejection of claim 4 is incorporated and further <u>PGP</u> teaches:

- the generating a secret value includes performing a Rivest-Shamir-Adleman (RSA) computation.

    (<u>PGP</u>, Page 22, Lines 2-5 "This version of PGP supports two distinct types of keys—the traditional RSA key used in older versions of PGP").

As per Claim 7: The rejection of claim 1 is incorporated and further <u>PGP</u> does not explicitly teach:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 4, Lines 18-21 "The secret key can be stored on the user's computer or in a special hardware device called a "Token". A special case of a Token is a "Smart Card" which is a credit card sized plastic card with a microprocessor chip embedded in the card. Smart Cards require a reader on the computer where access is made.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 8: The rejection of claim 7 is incorporated and further PGP does not explicitly teach:

- external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

However C.O.B.A.S. in analogous art does teach the above limitation.

(C.O.B.A.S., Page 4, Lines 18-21 as seen in the rejection of claim 7).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of C.O.B.A.S in to the teachings of Cisco, because one of ordinary skill in the art would be motivated to protect or insulate

authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 9: Claim 9 is the method claim of claim 1 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 12: The rejection of claim 9 is incorporated and further:

Claim 12 is the method claim of claim 4 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 4.

As per Claim 13: The rejection of claim 12 is incorporated and further:

Claim 13 is the method claim of claim 5 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claim 5.

As per Claim 15: The rejection of claim 9 is incorporated and further:

Claim 15 is the combination of the method claim of claim 7 and its dependent claim, claim 8 as a computer readable medium and is rejected under the same reasons as set forth in the rejection of claims 7 and 8.

As per Claim 30: Claim 30 is the method claim of claim 1 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 1.

As per Claim 32: The rejection of claim 30 is incorporated and further <u>PGP</u> teaches:

- means for encoding the shared secret using the public key received from the other node.

(<u>PGP</u>, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

Encrypting the single key inherently includes a means for encoding the shared secret (single key).

As per Claim 33: The rejection of claim 31 is incorporated and further:

Claim 33 is the method claim of claim 5 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 5.

As per Claim 34: The rejection of claim 30 is incorporated and further:

Claim 34 is the method claim of claim 8 as an apparatus and is rejected under the same reasons as set forth in the rejection of claim 8.

17. Claims 23,27,28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>PGP</u> in further view of <u>C.O.B.A.S.</u>.

As per Claim 23: <u>PGP</u> teaches:

- A protocol for establishing trust between two or more processing nodes

(<u>PGP</u>, Page 1, Lines 1-3 "With PGP™ for Personal Privacy, you can easily protect the privacy of your email messages and file attachments by encrypting them so that only those with the proper authority can decipher the information.").

- generating a public key and a private key on each of at least two nodes

(<u>PGP</u>, Page 21, Lines 6-8 "PGP is based on a widely accepted and highly trusted "public key encryption" system by which you and other PGP users generate a key pair consisting of a private key and a public key.").

- exchanging the public keys between the at least two nodes

(<u>PGP</u>, Page 21, Lines 9-11 "in order to correspond with other PGP users you need a copy of their public key and they need a copy of your public key.").

This inherently involves exchanging public keys.

- calculating a secret to be shared on at least one of the two nodes

(<u>PGP</u>, Page 91, Lines 12-13 "PGP uses a cryptographically strong pseudo-random number generator for creating temporary session keys.").

<u>PGP</u> does not explicitly teach:

- using an out-of-band mechanism comprising a computer-readable storage medium

However <u>C.O.B.A.S.</u> in analogous art does teach the above limitation.

(<u>C.O.B.A.S.</u>, Page 5, Paragraph 6 as seen in the rejection of claim 1)

The computers involved in the separate network have RAM.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of <u>C.O.B.A.S</u> in to the teachings of <u>Cisco</u>, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 27: The rejection of claim 23 is incorporated and further <u>PGP</u> teaches:

- encoding the secret to be shared using the public key from the other of the two nodes

(<u>PGP</u>, Page 21, Lines 17-19 "the data is encrypted using a much faster single-key algorithm, and it is this single key that is actually encrypted using the recipients public key.").

- transmitting the encoded secret to be shared to the other of the two nodes

(<u>PGP</u>, Page 22, Lines 26-58 "Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and certified e-mail is create a new key pair.").

(<u>PGP</u>, Page 22, Lines 2-5 "Anyone who has a copy of your public key can check your digital signature to confirm that you are the originator of the mail and that the contents have not been altered in any way during transit.").

<u>PGP</u> does not explicitly teach:

- via the out-of-band mechanism

However <u>C.O.B.A.S.</u> in analogous art does teach the above limitation.

(<u>C.O.B.A.S.</u>, Page 5, Paragraph 6 as seen in the rejection of claim 1)

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of <u>C.O.B.A.S</u> in to the teachings of <u>Cisco</u>, because one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks.

As per Claim 28: The rejection of claim 27 is incorporated and further <u>PGP</u> teaches:

- the calculating the secret to be shared includes performing an RSA calculation.

(<u>PGP</u>, Page 22, Lines 2-5 "This version of PGP supports two distinct types of keys—the traditional RSA key used in older versions of PGP").

As per Claim 29: The rejection of claim 23 is incorporated and further:

Claim 29 is the method claim of claim 8 as a protocol and is rejected under the same reasons as set forth in the rejection of claim 8.

18.   Claims 24,25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over (PGP). In further view of Cisco and C.O.B.A.S..

As per claim 24: The rejection of claim 23 is incorporated and further:

PGP does not explicitly teach:

- the calculating of the secret to be shared includes performing a function using the public key from the other of the two nodes and the private key.

However Cisco in analogous art teaches the above limitation.

(Cisco, Page 3, Line 36 "Alice computes $K_a = B^x \bmod n$.").

The generated secret value is K_a, X is the local private Key, B is the public key from other node.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Cisco in to the teachings of PGP and C.O.B.A.S., because one of ordinary skill in the art would be motivated to include a cryptographically strong equation in the generation of a pseudo-random single-key/session key.

As per claim 25: The rejection of claim 24 is incorporated and further <u>PGP</u> teaches:

- the calculating the secret to be shared includes performing a Diffie-Hellman calculation.

(<u>PGP</u>, Page 88, Lines 4-5 "PGP gives you the option of using keys based on the DSS/Diffie-Hellman encryption").

As per claim 26: The rejection of claim 24 is incorporated and further <u>PGP</u> teaches:

- the secret to be shared is symmetrical on the at least two nodes

(<u>PGP</u>, Page 88, Lines 9-13 "The PGP Symmetric Algorithms   PGP offers a selection of different secret-key algorithms to encrypt the actual message. By secret key algorithm, we mean a conventional, or symmetric, block cipher that uses the same key to both encrypt and decrypt.").

Conclusion

19.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.   Accordingly, **THIS ACTION IS MADE FINAL**.   See MPEP § 706.07(a).   Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-

270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
USPTO Customer Service Representative or access to the automated information
system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100